(5)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-039158
(43)Date of publication of application : 12.02.1999

(51)Int.Cl. G06F 9/06
G06F 12/14

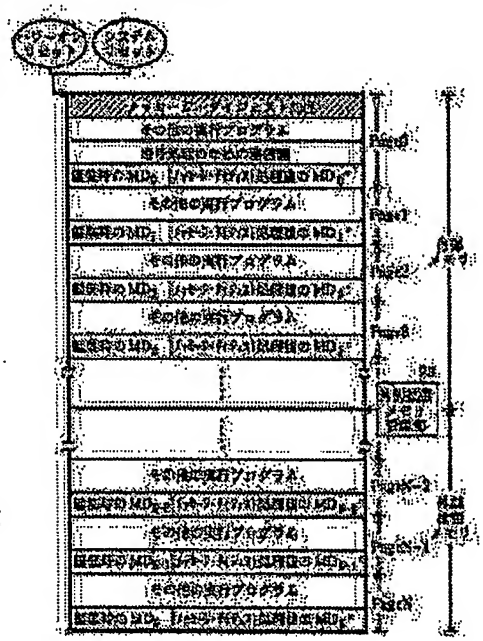
(21)Application number : 09-210006
(22)Date of filing : 18.07.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
N T T ELECTRON KK

(72)Inventor : KAWAKUBO HIDEJI
TAKADA SHUNSUKE
YAMANAKA KIYOSHI
MATSUMOTO HIROYUKI

(54) METHOD FOR PROTECTING EXECUTED PROGRAM AND ITS DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To stop reading of secret information of a processor itself by immediately stopping execution of an execution program when the execution program is detected to be forged before the specified execution program is run.
SOLUTION: A message digest processing is executed by branching a system into reset entry addresses of incorporated RUM/PROM after the system is reset. In this case, a message digest MD' is assigned to data byte obtained at the end of each processing. A message digest MD at editing is collated with the message digest MD' before which the message digest processing is executed whenever the execution program is run. And when the message digest MD at the editing and the message digest MD' after the message digest processing are not coincide, the execution program is judged to be forged and the execution of the execution program after that is stopped.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－39158

(43)公開日　平成11年(1999)２月12日

(51)Int.Cl.[6]		識別記号	FI		
G06F	9/06	550	G06F	9/06	550Z
	12/14	310		12/14	310Z

審査請求　未請求　請求項の数８　ＦＤ　（全 8 頁）

(21)出願番号　特願平9－210006

(22)出願日　平成９年(1997)７月18日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(71)出願人　591230295
エヌティティエレクトロニクス株式会社
東京都渋谷区桜丘町20番１号

(72)発明者　河久保　秀二
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　高田　俊介
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　川久保　新一

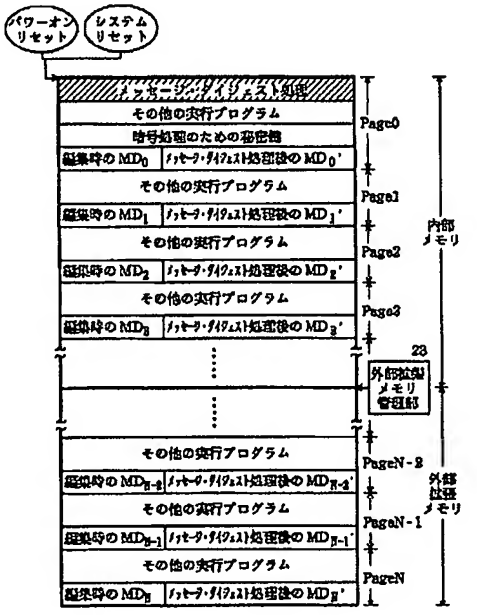
最終頁に続く

(54)【発明の名称】　実行プログラムの保護方法およびその装置

(57)【要約】

【課題】　１チップの中にＦＲＯＭ（フラッシュメモリ）等のＲＯＭとＲＡＭと処理部とが複合して構成されているＬＳＩにおいて、処理装置自身の秘密情報（秘密鍵）の読み出しを阻止することができ、また、悪意による処理装置の意図しない動作を阻止することができる実行プログラムの保護方法およびその装置を提供することを目的とするものである。

【解決手段】　パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出し、この改竄検出において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止するものである。



K4144

1

【特許請求の範囲】

【請求項１】　パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出段階と；上記改竄検出段階において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止段階と；を有することを特徴とする実行プログラムの保護方法。

【請求項２】　請求項１において、

上記所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み段階を有し、

上記改竄検出段階は、

上記実行プログラムを暗号処理する暗号処理段階と；上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第２のメッセージ・ダイジェストを抽出する第２のメッセージ・ダイジェスト抽出段階と；上記第２のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合段階と；上記メッセージ・ダイジェスト照合段階において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定段階と；によって構成されていることを特徴とする実行プログラムの保護方法。

【請求項３】　請求項２において、

上記編集時のメッセージ・ダイジェストは、上記暗号処理を実行しても変化しない態様で書き込まれていることを特徴とする実行プログラムの保護方法。

【請求項４】　パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と；上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段と；を有することを特徴とする実行プログラムの保護装置。

【請求項５】　請求項４において、

上記所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段を有し、

上記改竄検出手段は、

上記実行プログラムを暗号処理する暗号処理手段と；上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第２のメッセージ・ダイジェストを抽出する第２のメッセージ・ダイジェスト抽出手段と；上記第２のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と；上記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段と；によって構成されていることを特徴とする実行プログラムの保護装置。

2

【請求項６】　請求項５において、

上記編集時のメッセージ・ダイジェストは、上記暗号処理を実行しても変化しない態様で書き込まれていることを特徴とする実行プログラムの保護装置。

【請求項７】　パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と；上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段と；としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体。

【請求項８】所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段と；上記実行プログラムを暗号処理する暗号処理手段と；上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第２のメッセージ・ダイジェストを抽出する第２のメッセージ・ダイジェスト抽出手段と；上記第２のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と；上記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段と；上記改竄判断手段において上記改竄が判断されると、上記実行プログラムの実行を直ちに停止する実行停止手段と；としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、実行プログラムを保護する方法およびその装置に関する。

【０００２】

【従来の技術】従来、パーソナルコンピュータや、パーソナルコンピュータの拡張バスに画像処理・音声処理等の専用制御ボード等が接続され、上記専用制御ボード等において、これらの処理や制御を実行するＣＰＵと、プログラムの実行メモリ（ＲＡＭ）と、実行プログラムの保管や処理開始時や実行中に読み出し／書き込みされるデータメモリ（ＲＯＭ）とが、互いに別々に構成され、バスによって接続される構成が採用されている。

【０００３】上記構成においては、上記実行メモリ、上記データメモリの内容を、実行プログラムの実行前に、部分的に変更することが可能である。したがって、実行メモリ、データメモリの内容を、実行プログラムの実行前に、第三者が部分的に変更すれば、上記実行プログラムの実行する処理装置自身の秘密情報（秘密鍵）を読み出すことが可能であり、また、上記処理装置における意図しない動作を、第三者が外部から強制的に実行させることが可能である。

【０００４】

【発明が解決しようとする課題】図５は、従来の画像処理・音声処理等の専用制御ボードＣＢ１を示すブロック図である。

【０００５】画像処理・音声処理等の専用制御ボードＣＢ１は、処理部（ＣＰＵ）１１と、データメモリとしてのＲＯＭ１２と、実行メモリとしてのＲＡＭ１３とを１チップに封入したものである。なお、符号１４は、インタフェース部であり、符号１５は、カードＩ／Ｆ部である。

【０００６】このように、実行メモリとデータメモリと処理部とを１チップ化することによって、上記処理装置自身の秘密情報（秘密鍵）が伝送される信号線は、上記チップの外部に露出しないので、第三者が、チップの外部において、信号線に端子等を接触させ、上記秘密情報（秘密鍵）を取り出す操作を実行することは不可能である。

【０００７】つまり、上記の場合、信号線に端子等を接触させ、上記秘密情報（秘密鍵）を取り出す操作を実行するためには、チップのケースを開く必要があり、そのケースを開いたとしても、チップ内部の配線のうちでどの配線に端子等を接触させればよいかの判断が極めて困難であり、また、端子等を接触させるべき配線が分かったとしても、チップ内部の微細な配線に端子等を接触させることが実際上不可能である。したがって、上記処理装置自身の秘密情報（秘密鍵）の読み出しを阻止することができ、また、外部からの悪意による処理装置の意図しない動作を阻止することができる。

【０００８】しかし、上記のように１チップ化したとしても、ＲＡＭ１３の内容をコピーすれば、上記処理装置自身の秘密情報の読み出しを阻止することができないという問題がある。

【０００９】また、上記のように１チップ化したとしても、製造工程で用いるＲＯＭ書き込み装置を利用して、ＲＯＭ１２の内容を改竄した場合や、ＲＡＭ１３を部分修正した場合には、外部からの悪意による処理装置の意図しない動作を阻止することができないという問題がある。

【００１０】本発明は、１チップの中にＦＲＯＭ（フラッシュメモリ）等のＲＯＭとＲＡＭと処理部とが複合して構成されているＬＳＩにおいて、処理装置自身の秘密情報（秘密鍵）の読み出しを阻止することができ、また、悪意による処理装置の意図しない動作を阻止することができる実行プログラムの保護方法およびその装置を提供することを目的とするものである。

【００１１】

【課題を解決するための手段】本発明は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出し、この改竄検出において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止するものである。

【００１２】

【発明の実施の形態および実施例】図１は、本発明の一実施例である実行プログラムの保護装置ＰＰ１を示すブロック図である。

【００１３】実行プログラムの保護装置ＰＰ１は、ＣＰＵ等で構成されている処理部２１と、データメモリとしてのＲＯＭ２２と、実行メモリとしてのＲＡＭ２３と、インタフェース部１４と、カードＩ／Ｆ部１５と、拡張ＲＯＭ２４と、拡張ＲＡＭ２５と、外部拡張メモリ管理部２６とを有するものである。

【００１４】また、実行メモリとしてのＲＡＭ２３と、データメモリとしてのＲＯＭ２２と、処理部２１と、インタフェース部１４と、外部拡張メモリ管理部２６とは、図１において太線で囲まれており、この太線内の素子が１チップ化されている。

【００１５】処理部２１は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段の例であり、上記改竄検出段階において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段の例である。また、処理部２１は、上記所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段の例である。

【００１６】なお、「メッセージ・ダイジェスト」は、メッセージ・ダイジェストの対象となる原文（上記実施例においては、実行プログラム）が１ビットでも書き換えられると、その原文についてメッセージ・ダイジェスト処理を実行した後に、変化するものである。

【００１７】さらに、上記改竄検出手段は、上記実行プログラムを暗号処理する暗号処理手段と、上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第２のメッセージ・ダイジェストを抽出する第２のメッセージ・ダイジェスト抽出手段と、上記第２のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と、上

記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段とによって構成され、これらの各手段も、処理部２１が実現する。なお、上記編集時のメッセージ・ダイジェストは、上記暗号処理を実行しても変化しない態様で書き込まれている。

【００１８】ここで、「メッセージ・ダイジェスト」は、上記実施例においては、一方向性ハッシュ関数によって実行プログラムを処理した後における最後の１６バイトのデータであり、「メッセージ・ダイジェスト処理」は、一方向性ハッシュ関数によって実行プログラムを処理する動作である。上記一方向性ハッシュ関数のアルゴリズムとしては、ＭＤ２、ＭＤ５、ＳＨＡ－１等があり、これらのうちのどのアルゴリズムを使用してもよい（ＭＤ２、ＭＤ５、ＳＨＡ－１については、「『暗号理論入門』　岡本栄司著　共立出版株式会社」を参照）。また、上記一方向性ハッシュ関数以外の関数を使用して実行プログラムを処理することによって、メッセージ・ダイジェストを実現するようにしてもよい。

【００１９】図２は、上記実施例におけるメモリマップを示す図である。

【００２０】図２に示すメモリマップは、ＲＡＭ２３の内部メモリの領域と、拡張ＲＡＭ２５の外部拡張メモリの領域とが使用され、Page０～PageＮで構成されている。

【００２１】Page０には、メッセージ・ダイジェスト処理のプログラムと、その他の実行プログラムと、暗号処理のための秘密鍵と、Page０に関する編集時のメッセージ・ダイジェストMD_0と、Page０に関するメッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD_0'とが格納されている。

【００２２】なお、メッセージ・ダイジェスト処理する場合、上記のように、ＭＤ２、ＭＤ５、ＳＨＡ－１等のうちのどのアルゴリズムを使用してもよいが、所定Pageについて編集時のメッセージ・ダイジェストを生成する場合に使用するアルゴリズムと、所定Pageについて実行プログラムを走行させる前にそのPageおいてメッセージ・ダイジェスト処理する場合に使用するアルゴリズムとが同一である必要がある。

【００２３】Page１には、その他の実行プログラムと、Page１に関する編集時のメッセージ・ダイジェストMD_1とが格納されている。また、メッセージ・ダイジェスト処理後には、Page１に関するメッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD_1'が、Page１に格納される。

【００２４】Page２以降の各Pageには、Page１における内容と同様の内容が格納され、その他の実行プログラムと、そのPageに関する編集時のメッセージ・ダイジェストとが格納され、また、メッセージ・ダイジェスト処理後には、そのPageに関するメッセージ・ダイジェスト処理後のメッセージ・ダイジェストが、そのPageに格納される。

【００２５】なお、メッセージ・ダイジェスト処理は、アルゴリズムを明示しないメッセージ・ダイジェスト処理であり、各Pageのメッセージ・ダイジェストを作成する機能を有し、Page０のメッセージ・ダイジェスト処理は、各Pageのメッセージ・ダイジェストをとる。つまり、図２には、Page０にのみメッセージ・ダイジェスト処理が記載されているが、Page１以降の各Pageにおいてメッセージ・ダイジェスト処理が実行される。

【００２６】また、「実行プログラム」は、たとえば電文を外部から読み込む処理や、その読み込んだ電文に暗号処理を施す処理を記述したプログラムである。さらに、「その他の実行プログラム」は、メッセージ・ダイジェスト処理のプログラム以外の実行プログラムである。

【００２７】次に、上記実施例の動作について説明する。

【００２８】図３は、上記実施例において、実行プログラムの保護装置ＰＰ１を製造するときにおける動作を示すフローチャートである。

【００２９】まず、Pageの関数ｎを「０」とし（Ｓ１）、Page ｎに書き込むべき実行プログラムをロードする（Ｓ２）。そして、編集時のメッセージ・ダイジェストMD_nを生成し（Ｓ３）、上記編集時のメッセージ・ダイジェストMD_nを、該当Pageの最後の１６バイトに書き込む（Ｓ４）。

【００３０】次に、Page ｎに書き込むべき実行プログラムについてメッセージ・ダイジェスト処理を実行することによってメッセージ・ダイジェストMD_n'を生成し（Ｓ５）、１Page分のプログラムをメモリ２３に書き込み、その書き込まれた内容を編集する（Ｓ６）。そして、編集された内容をPage単位でＰＲＯＭ２２に書き込み（Ｓ７）、次のPageについて上記処理（Ｓ２～Ｓ７）を実行し（Ｓ８、Ｓ９）、最大のPageＮまで上記処理（Ｓ２～Ｓ７）が終了すると、実行プログラムの保護装置ＰＰ１を製造する場合における全ての処理を終了する。

【００３１】次に、上記実施例における実行プログラムの保護動作について説明する。

【００３２】図４は、上記実施例における実行プログラムの保護動作を示すフローチャートである。

【００３３】まず、電源投入時にパワーオンリセットする（Ｓ１１）か、または、システムリセットした（Ｓ１２）後に、内蔵のＲＯＭ／ＰＲＯＭ２２のリセット・エントリ・アドレスに分岐し、メッセージ・ダイジェスト処理を実行する（Ｓ２１）。なお、各処理の最後に得られるデータ１６バイトに、上記メッセージ・ダイジェストMD'を割り当てる。

【００３４】編集時のメッセージ・ダイジェストMD

と、実行プログラムを走行する毎に、その直前にメッセージ・ダイジェスト処理が行われたメッセージ・ダイジェストMD'とを、照合手段（図示せず）が照合する（Ｓ２２、Ｓ２４～Ｓ３１）。そして、この照合の結果、上記予め作成されている編集時のメッセージ・ダイジェストMDと、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'とが、全てのPageにおいて一致した場合にのみ、上記実行プログラムの動作を通常通りに開始させる。

【００３５】すなわち、実行プログラムに変化が加えられていなければ（改竄されていなければ）、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'が変化しないので、このメッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'は、編集時のメッセージ・ダイジェストMDと同じである。

【００３６】一方、上記照合の結果、編集時のメッセージ・ダイジェストMDと、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'とが一致しなかった場合（Ｓ２２、Ｓ２４、Ｓ３２）、実行プログラムが変化されている場合であり、多くの場合、その実行プログラムが改竄されているので、その段階で、実行プログラムの実行を停止する。編集時のメッセージ・ダイジェストMDと、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'とが一致しなかった場合、その実行プログラムが改竄されたと判断し、その後の実行プログラムの実行を停止する。

【００３７】このようにすることによって、１チップの中にＦＲＯＭ（フラッシュメモリ）等のＲＯＭとＲＡＭと処理部とが複合して構成されているＬＳＩにおいて、実行プログラムが改竄されたと判断されると、その後の実行プログラムの実行を停止するので、処理装置自身の秘密情報（秘密鍵）の読み出しを阻止することができ、また、悪意による処理装置の意図しない動作を阻止することができる。

【００３８】実行プログラムが大規模であれば、上記実施例のように外部拡張メモリを使い、この場合、命令によって、メモリ拡張モード・レジスタを設定する。このようにすることによって、外部メモリ領域に外部デバイスを接続できる外部拡張モードになる。

【００３９】上記実施例において、実行プログラムが大規模でなければ、拡張ＲＯＭ２４、拡張ＲＡＭ２５、外部拡張メモリ管理部２６を省略するようにしてもよい。

【００４０】上記実施例を、装置の発明として把握すると、上記実施例は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と、上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段とを有する実行プログラムの保護装置である。

【００４１】この場合、所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段を有し、上記改竄検出手段は、上記実行プログラムを暗号処理する暗号処理手段と、上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第２のメッセージ・ダイジェストを抽出する第２のメッセージ・ダイジェスト抽出手段と、上記第２のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と、上記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段とによって構成されている。

【００４２】また、上記実施例を、記録媒体の発明として把握すると、上記実施例は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と、上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段ととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体である。

【００４３】この場合、所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段と、上記実行プログラムを暗号処理する暗号処理手段と、上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第２のメッセージ・ダイジェストを抽出する第２のメッセージ・ダイジェスト抽出手段と、上記第２のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と、上記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段と、上記改竄判断手段において上記改竄が判断されると、上記実行プログラムの実行を直ちに停止する実行停止手段ととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体である。

【００４４】

【発明の効果】本発明によれば、１チップの中にＦＲＯＭとＲＡＭと処理部とが複合して構成されているＬＳＩにおいて、処理装置自身の秘密情報の読み出しや、悪意による処理装置の意図しない動作を排除することができるという効果を奏する。

9

【図面の簡単な説明】

【図１】本発明の一実施例である実行プログラムの保護装置ＰＰ１を示すブロック図である。

【図２】上記実施例におけるメモリマップを示す図である。

【図３】上記実施例において、実行プログラムの保護装置ＰＰ１を製造するときにおける動作を示すフローチャートである。

【図４】上記実施例における実行プログラムの保護動作のフローチャートである。

10

【図５】従来における画像処理・音声処理等の専用制御ボードＣＢ１を示すブロック図である。

【符号の説明】

ＰＰ１…実行プログラムの保護装置、

２１…処理部、

２２…ＲＯＭ／ＰＲＯＭ、

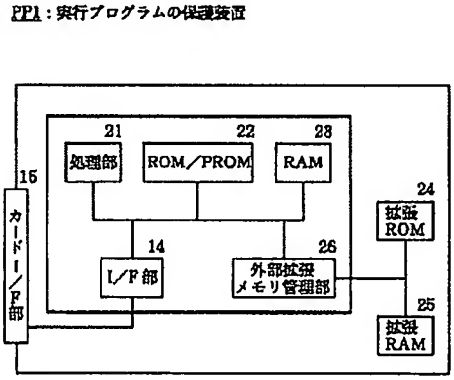
２３…ＲＡＭ、

２４…拡張ＲＯＭ、

２５…拡張ＲＡＭ、

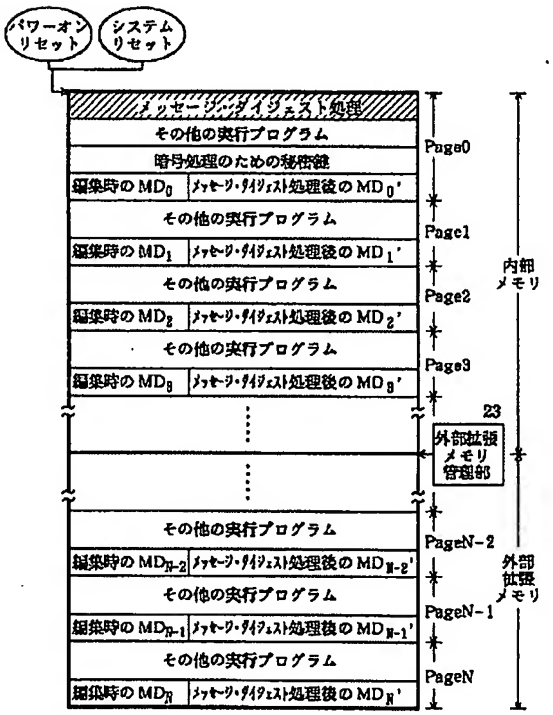
２６…外部拡張メモリ管理部。

【図１】



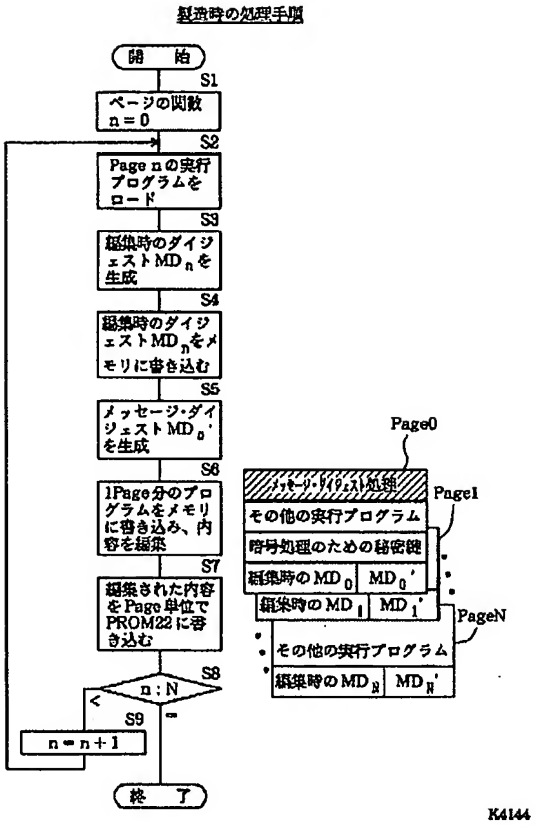
K4144

【図２】

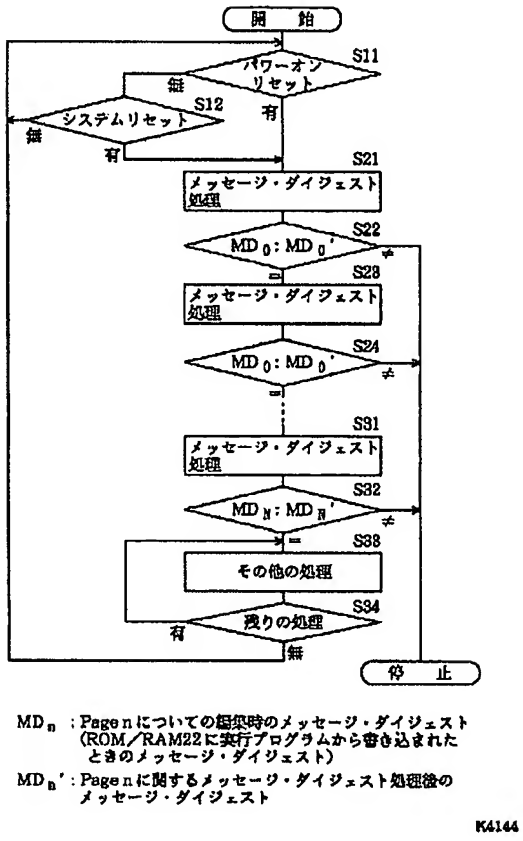


K4144

【図３】



【図４】

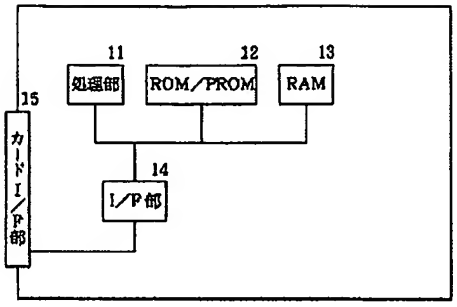


MD n ：Page nについての編集時のメッセージ・ダイジェスト（ROM／RAM22に実行プログラムから書き込まれたときのメッセージ・ダイジェスト）

MD n ' ：Page nに関するメッセージ・ダイジェスト処理後のメッセージ・ダイジェスト

【図５】

CB1：従来の専用制御ボード



K4144

フロントページの続き

(72)発明者　山中　喜義
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　松本　博幸
東京都渋谷区桜丘町20番１号　エヌティティエレクトロニクス株式会社内